OCR

Oxford Cambridge and RSA

Wednesday 17 January 2024 – Morning

Level 3 Cambridge Technical in IT

05839/05840/05841/05842/05877 Unit 3: Cyber security

Time allowed: 1 hour

C384/2401

You must have:
- a clean copy of the Pre-release (inside this document)

INSTRUCTIONS
- Use black ink.
- Write your answer to each question in the space provided. If you need extra space use the lined pages at the end of this booklet. The question numbers must be clearly shown.
- Answer **all** the questions.
- Use the Insert to answer the questions in Section A.

INFORMATION
- The total mark for this paper is **60**.
- The marks for each question are shown in brackets **[ ]**.
- Quality of extended response will be assessed in questions marked with an asterisk (*).
- This document has **12** pages.

ADVICE
- Read each question carefully before you start your answer.

Section A

1 PH Virtual Challenges suspects that its organisation's data is being stolen by an insider.

(a)
(i) Explain why PH Virtual Challenges needs to **protect** its organisation's data.

....

....

....

....

....

.... **[3]**

(ii) Explain, using an example, how **escalation of privileges** could be used by an insider at PH Virtual Challenges to gain unauthorised access to data.

....

....

....

....

....

.... **[3]**

(b) PH Virtual Challenges suspects the insider is **stealing** customer data.

(i) Identify **three** different ways that an insider could **steal** customer data from the network.

Way 1 ....

....

Way 2 ....

....

Way 3 ....

....

[3]

(ii) Describe **two** different ways that the theft of data can impact the **safety** of the customer.

Way 1 ....

....

....

....

Way 2 ....

....

....

....

[4]

(iii)* Discuss the **impact** of a loss of data for PH Virtual Challenges.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

.... **[10]**

2 PH Virtual Challenges has identified that it has been subjected to a **system attack**.

(a) Explain, using an example, what a **system attack** means.

....

....

....

....

....

.... **[3]**

(b) Describe why an attack on the data held by PH Virtual Challenges might be **state sponsored**.

....

....

....

.... **[2]**

Turn over

3 When responding to a cyber security incident, PH Virtual Challenges follows a **handbook**.

(a)
(i) Why is it **important** to list the responsibilities of individuals in the **handbook**?

....

.... **[1]**

(ii) Why is it **important** to list the individuals to contact in the **handbook**?

....

.... **[1]**

(iii) Why is it **important** to list the procedures to be followed in the **handbook**?

....

.... **[1]**

(iv) Why is it **important** to know the **extent** of the incident?

....

.... **[1]**

(b) Following a cyber security incident, PH Virtual Challenges completes a **Cyber Security Incident Report** (CSIR).

(i) **Complete** the following sentences using the list of words below.

Not all words need to be used.

- Attacker
- Category
- Characteristics
- Incident
- Motivation
- Techniques

The CSIR needs to record the type of _____ so that they

can understand their _____ .

The CSIR will record the _____ used by the attacker.

[3]

(ii) Explain why the CSIR needs to **include** identification of trends.

....

....

....

....

....

.... **[3]**

(iii) Explain why, following a cyber security incident, the section in the CSIR on recommendation of changes might **not** contain any recommendations.

....

....

....

.... **[2]**

Turn over

Section B

You do **not** need the case study to answer these questions.

Taylor has become concerned about their personal security.

4

(a) Taylor has installed a security alarm in their house. When activated it gives out a high-pitched continuous sound.

Describe **one advantage** and **one disadvantage** of the use of a security alarm.

Advantage ....

....

....

....

Disadvantage ....

....

....

....

[4]

(b) Taylor uses their fingerprint to unlock and access their phone.

Explain the process carried out when **biometrics** are used to unlock and access the phone.

....

....

....

....

....

....

....

.... **[4]**

(c) Explain how Taylor could make use of an **intrusion detection system** (IDS) on their home network.

....

....

....

....

....

.... **[3]**

5 Give **two** ways **organised crime** could target Taylor's phone.

Way 1 ....

....

Way 2 ....

....

[2]

Turn over

6* Explain how Taylor could use cyber security risk management to protect their **digital vulnerabilities**.

....

....

....

....

....

....

....

....

....

....

....

....

.... **[7]**

END OF QUESTION PAPER

EXTRA ANSWER SPACE

If you need extra space use this lined page. You must write the question numbers clearly in the margin.

C384/2401